Amendments to the Specification:

Amend page 27, second full paragraph (lines 13-18) to read as follows:

Poly_B0 = x^8 ⊕ α^**92** ⊗ x^7 ⊕ α^**229** ⊗ x^6 ⊕ α^**5** ⊗ x^5 ⊕ α^**95** ⊗ x^4 ⊕ α^**84** ⊗ x^3 ⊕ **0** ⊗ x^~~3~~2 ⊕ α^**195** ⊗ x ⊕ α^**176,** where α(X) = α = X to obtain the 8-tuple $j_7X^7 + j_6X^6 + j_5X^5 + j_4X^4 + j_3X^3 + j_2X^2 + j_1X + j_0$. The values for the individual coefficient multipliers are as follows:

Amend page 33, last paragraph (lines 12-17) to read as follows:

The non-linear mix functions 161, 162 used to combine two bytes shifted directly from the register A or register B (RGA_2/RGA_4, RGB_3/RGB_5) with others that are from the F1 tables:

$g0 = RGA'_{0|7} \otimes RGB'_{1|6} \oplus RGA_2 \otimes RGB'_4 \oplus RGA'_5 \otimes RGB_3$

$g1 = RGA'_{1|6} \otimes RGB'_{0|7} + RGA_4 \otimes RGB'_2$ [+]⊕ $RGA'_3 \otimes RGB_5$

Amend page 35, first full paragraph (lines 4-16) to read as follows:

The S-box is initialized linearly to $S_0 = 0$, $S_1 = 1$, …, $S_{255} = 255$. The S-box permutation process can be formulated in accordance with the following relationships:

n from 0 to runup_Cycles

n = (n % 256);

Y0' = (g0 + ~~$S_{RGB7|0}$~~ $S_{RGB0|7}$ + S_n) mod 256

swap S_i and $S_{Y0'}$

Y1' = (g1 + ~~$S_{RGA7|0}$~~ $S_{RGA0|7}$ + S_n) mod 256

swap S_i and $S_{Y1'}$

t0 = (S_{g1} + $S_{Y0'}$) mod 256

t1 = (S_{g0} + $S_{Y1'}$) mod 256

Y0 = S_{t0} and Y1 = S_{t1}